
Systems and Risk Analysis for Food Protection and Security

DETLOF VON WINTERFELDT

*International Institute for Applied Systems Analysis
Laxenburg, Austria*

detlof@iiasa.ac.at

As I put this presentation together, I reflected on the two streams of research that I have pursued for the past decade. One is systems analysis which is my current job and the other is risk analysis. I serve as director for CREATE, the National Center for Risk and Economic Analysis of Terrorism Events at the University of Southern California, the first center of excellence funded by the Department of Homeland Security. Of course, Minnesota is home to the second center of excellence, the National Center for Food Protection and Defense, which is represented here by Director Emeritus Frank Busta. At CREATE, our primary focus is on risk analysis applied to terrorism and most of my examples are from that area. Since 2009, I have been the director also of the International Institute for Applied Systems Analysis (IIASA) in Laxenburg, Austria. There, our tools are forms of modeling applied to global problems, including the major theme of water security. Other themes are energy, climate change and policy. I will outline systems analysis and risk analysis, and provide three examples, and prioritize some terrorism issues.

SYSTEMS ANALYSIS

Why systems analysis? Here are quotes by Larry Summers¹ from 2009 after reading *Decision Analysis* by Howard Raiffa, IIASA's first director:

Many children were taught to believe in God, I came to believe in the power of systems analysis.

¹The 71st United States secretary of the treasury from 1999 to 2001 under President Clinton, and director of the National Economic Council for President Obama until November 2010.

and from the *IIASA Strategic Plan 2011–2020*:

Today, policymakers around the globe ask for problem-focused, solution-oriented, interdisciplinary research to help them with their complex decisions. They may not know it, but they are really asking for systems analysis.

Systems analysis is a group of model-simulation analysis tools—applied mathematics if you will—specifically applicable to very complex systems that undergo dynamic changes and are fraught with uncertainty. A classic example of a problem that lends itself to systems analysis is the collapse in the financial system, which indicated many of those features and which we are not very good at modeling. Ecosystems are another area where we are applying it, energy systems, food production, and so on. All of this is applied mathematics, but, more importantly, it is guided by some major overriding factors: the analysis should be problem-focused and solution-oriented. You start with the problem. You don't start with a mathematical model and look for a problem, and you look for solutions, not necessary optimal solutions but acceptable solutions, and eliminate poor solutions. The model is usually developed by a multidisciplinary team taking a holistic view of the problem.

RISK ANALYSIS

Why risk analysis? Michael Chertoff² has stated the following in several versions:

We have to identify and prioritize risks—understanding the threat, the vulnerability and the consequence. And then we have to apply our resources in a cost-effective manner.

Frequently, I use that quote to motivate risk analysis. It's what risk analysis is supposed to do, *i.e.* help decision-makers. It is a combination of risk assessment and management that involves identifying the risks, quantifying them—*i.e.* quantifying the possibilities of events that could occur as well as quantifying their consequences—and then looking at decision-opportunities, intervention and risk reduction, and evaluating them. The tools that we use in risk analysis are on one level just formal expert elicitation of probabilities. Often event trees and fault trees, Bayesian networks and influence diagrams are used. The combination of systems analysis and risk analysis can move us forward in a qualitative step when we need them for problems like systemic risk in the financial sector, ecosystem risk, food risk, and so on.

CHALLENGES OF TERRORISM

Terrorism imposes particular challenges. Terrorists tend to search for high vulnerabilities and consequences, unlike technological or natural disasters that occur randomly. They observe our defenses and try to attack the weakest remaining links, then change their modes and targets of attack. They also try to create events that produce ripple effects through instilling fear and eliciting behavior change that can be more damaging than the direct results of the event. For example, the direct cost of 9/11 was \$20 million to \$30

²Second United States secretary of homeland security under Presidents G.W. Bush and Obama.

billion, including insurance for lives lost, whereas the indirect costs were more like \$200 billion, due to reduction of air-travel, *etc.*

Several attempts have been made to apply risk analysis to terrorism—probabilistic risk analysis, event trees and elicitation of expert probabilities. More recently, decision-tree analysis has been employed and game theory—attacker-defender games and experimental games—as well as vulnerability and risk-scoring systems.

Lugar Report

Three years ago, Senator Lugar conducted a survey of eighty people, for their opinions of the probabilities of a major attack, *i.e.* nuclear, biological, chemical or radiological, somewhere in the world (Figure 1).

Event	Median Probability (5 Years)	Median Probability (10 Years)	Appr. Sample Size
Nuclear Attack	10%	20%	80
Biological Attack	10%	20%	80
Chemical Attack	15%	15%	80
Radiological Attack	25%	40%	80

Figure 1. Lugar report informal expert elicitation.
Survey of probabilities of major attacks.

The median probability of a nuclear or biological attack was judged to be 10% in the next 5 years and 20% in the next 10 years, and more so for chemical and radiological attacks. I think that these numbers are too high and we can do better. Those surveyed were prominent people from Harvard, the CIA, the Senate, the military, *etc.*, but I would argue that they weren't the right people to answer that question. We should be using the right experts, asking the right questions and using the right procedures (Figure 2).

Bioterrorism Risk Assessment

In an exercise in the context of bioterrorism risk assessment for the Department of Homeland Security (DHS), we tried to do things better. This was in the context of the DHS biannual report to the president, particularly to prioritize biological events and guide investments for risk management. CREATE provided help with expert elicitation for threat assessment. We began by creating a list of twenty-eight biological agents that were prioritized by intelligence analysts and social scientists to provide probability assessments of threats and risks, and also of consequences. We helped the development of elicitation protocols and gave them tools, and while we didn't do the actual elicitation—which was highly classified—mostly we tried to find elicitors, the people who did the work, and we

provided software support. We also made sure that they were able to quantify uncertainties in their assessments. Most of the intelligence analysts that I have worked with in the past say, “It’s probably between 5% and 20%”; so, we helped them to be more specific in terms of setting their probability distributions.

➤ **Use the right experts**

- ❖ Intelligence analysts
- ❖ Social scientists studying terrorists behavior
- ❖ Journalists

➤ **Ask the right questions**

- ❖ Create a complete set of attack scenarios
- ❖ Ask about motivations and capabilities
- ❖ Ask for relative likelihoods

➤ **Use the right procedures**

- ❖ Train experts and provide practice
- ❖ Use state-of the art elicitation protocols
- ❖ Document carefully

Figure 2. Possible improvements over the Lugar survey.

Figure 3 provides a hypothetical, but relatively realistic, example of a result. Certain infectious agents are generally found at the top of such probability assessments. For example, this particular operation estimated roughly a 25% chance of an event involving *Bacillus anthracis* (anthrax) in the next 10 years and a 13% chance of an event involving *Yersinia pestis* (bubonic plague), botulinum toxin or ricin occurring in the next 10 years. These are cases where there is some bias towards events that have already happened. An important aspect is that only four to seven biological agents are deemed most dangerous, and many are assigned low probabilities although not necessarily for good reasons. Figure 4 is an example from the report, unlabelled because the information is classified, showing agents of high, medium and low risk. This was used in the first report to the president in 2006 and in the second in 2008, and I assume it was in the 2010 report, but I was already at IIASA then. This provides a reasonable first baseline on risk assessment, but it needs to have a closer tie to risk management. We need to figure out how these numbers change with interventions and that was not done in the parts that I was involved in, but I understand that there is some effort in that direction now. Also, we need to go beyond event trees to model complex systems, and we need to consider terrorists’ shifting tactics.

Hi Lethal - Comm	RP
Yersinia pestis *	13%
Variola Major Virus	1%
Ebola	6%
Lassa	6%
Marburg	6%
Hi Lethal- Non Comm	
Bacillus anthracis *	25%
Clostridium botulinum *	13%
Ricinus communis (castor bean)	13%
Burkholderia mallei	1%
Nipah virus	1%
Bovine Spongiform Encephalopathy *	1%
Vibrio cholerae **	3%
Other Agents	9%

Figure 3³. Relative probabilities (RP) of selected agents
(given a bioterrorism attack—hypothetical expert).

Systems with Interdependencies

Los Angeles airport and Long Beach harbor are complex systems that involve people movement and supply chains, and fully protecting them is tricky because necessary resources are lacking. So, decisions were needed as to where to place defensive resources. One of our ideas that worked well was to use smart randomization. Everything can be protected by employing a randomization scheme to protect valuable targets randomly and thus confuse terrorists. Accordingly, patrols, inspections and surveillance are randomized. A student of ours came up with a wonderful idea to use a Stackelberg game—a business game—also called a leader-follower game. He developed a game that involves a defender and an attacker and two assets, asset A and asset B where asset A is more valuable than asset B. If only asset A is protected then the attacker will attack asset B because he will know that you protect asset A and then you lose and the attacker gains. If the attacker is stupid and attacks A while you are protecting A then you win and the attacker loses. In contrast, if you protect B the attacker will attack A and not B. To solve this zero-sum game, you can randomize between A and B and thereby find a way to get the attacker to achieve the minimum expected value. In our analysis, we extended this to non-zero-sum games, multiple targets, multiple attackers, with certain real-world constraints—patrol personnel have to eat sometime, somewhere—with fast algorithms and real-world implementation.

³Comm = communicable; Non Comm = noncommunicable.

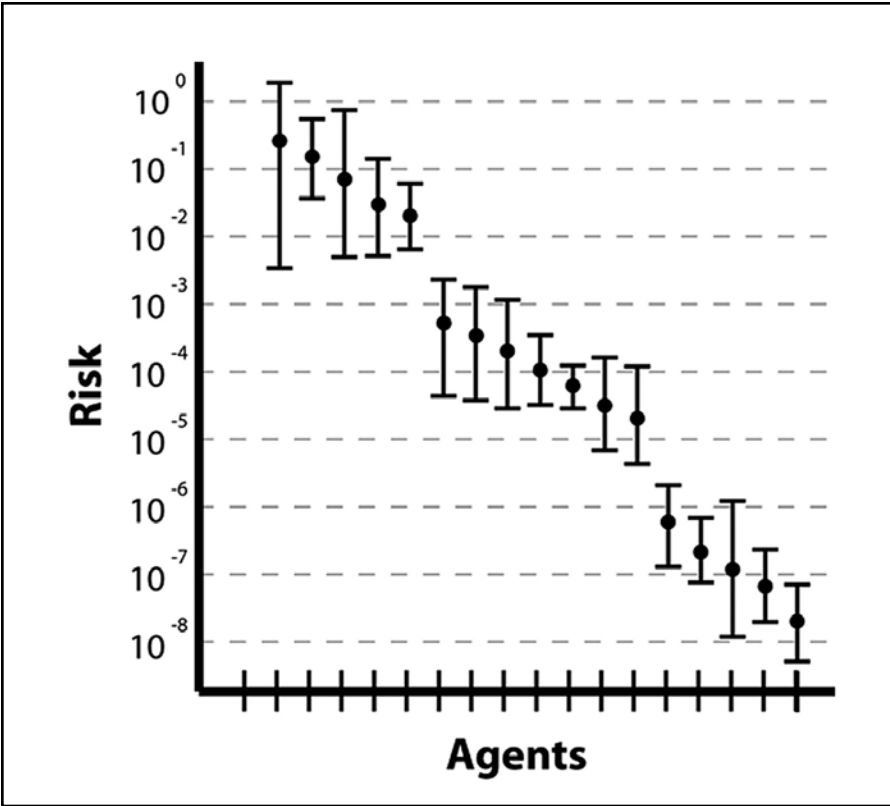


Figure 4. Biological agents (classified) of high, medium and low risk on a relative scale.

The assistant for randomized monitoring over routes (ARMOR) project was implemented in cooperation with the Los Angeles Police Department which provided inputs into ARMOR which were randomized by the game-theory algorithm and the randomized schedule was then given back to the police. There was some override capability because flexibility is essential, but they never did change it during the first two years of operation. ARMOR is still being used at the airport and there is statistical evidence that the intervention rates a LAX improved substantially after the system was implemented. It is now used also by the TSA to randomize the assignment of federal marshals on airplanes, and other projects.

COMBINING SYSTEMS FOR FOOD PROTECTION

My last example illustrates combining systems and risk analyses for food protection. The initial idea was to formulate a model of the food-supply chain and then to superimpose a risk model. Although this is an elegant approach, it is also cumbersome. But, once you

have a model of the food-supply chain, the threats, vulnerabilities and consequences can be assessed as can baseline risks. Then protective measures can be identified, including optimal sampling procedures, inspections and randomized patrols. Figure 5 shows a relatively simple supply chain, *i.e.* for milk in Minnesota, starting with the cow and ending in the grocery store, and passing through many stages. (On the other hand, the supply chain for a hamburger is much more complicated.) There are many storage and testing locations and transportation stages, *etc.*, and when they are mapped out a mathematical model of the flow may be constructed, and points of vulnerability may be identified (Figure 5).

A terrorist attack would most likely occur close to the end of the supply chain, depending on the volume of material; the larger the volume the less likely the intervention will be detected. With a deterministic model—looking at attack modes, for example introducing pathogens, radionuclides or chemicals into the process—come indicators of deaths, both acute and delayed, illnesses, and direct and indirect economic costs. This is less of a risk analysis, and essentially a systems-analysis model, and an advantage of turning it into a computer model is that we can allow the user to adjust the input parameters through sliders and scrollbars in Excel.

The next steps with risk analysis are to identify the highest risks and risk-management options, assess uncertainty over systems-model parameters—like uncertainty over LD_{50} , or uncertainty over mode of attack—then assess probabilities of attacks with and without risk management and conduct cost-benefit analysis of risk-management options.

Risk Transfer

The discussion above applies to just one supply chain, raising the issue of the enormity of the task of doing this for all supply chains, comprising many kinds of complicated food products. Another complication is the problem of risk transfer, because terrorists can observe our defenses. On the other hand, if they don't observe our defenses it may be that they should be told, so that they won't want to go there. But, once they know, they will adapt and change modes and attack other targets, so risks will be shifted to less-defended parts of the system and the overall risk level may change little. Nuclear detection and nuclear defense provide a good example. You can put radionuclide-detection portals around the United States at main entry points, but terrorists will find holes in the system as do smugglers entering the United States from Mexico and Canada. That is a significant problem.

Further to risk transfer: within a given system—*e.g.* a supply chain for a food item—risk transfer can be analyzed. Once you have plugged one vulnerability, you can then see how the risk shifts to another vulnerability. In theory, you can plug many of them and stop at a point where it is no longer cost-effective. Across systems, where there are multiple supply chains for a food item, it is harder. And for multiple food items and multiple supply chains, the task becomes daunting. We need a bottom-up approach, which is the one that I just described, in connection with a top-down approach to provide a holistic view of the food type and the pathogen or chemical that a terrorist might use. However, working both from the bottom and from the top and hopefully finding appropriate linkages will be time consuming and involve much effort.

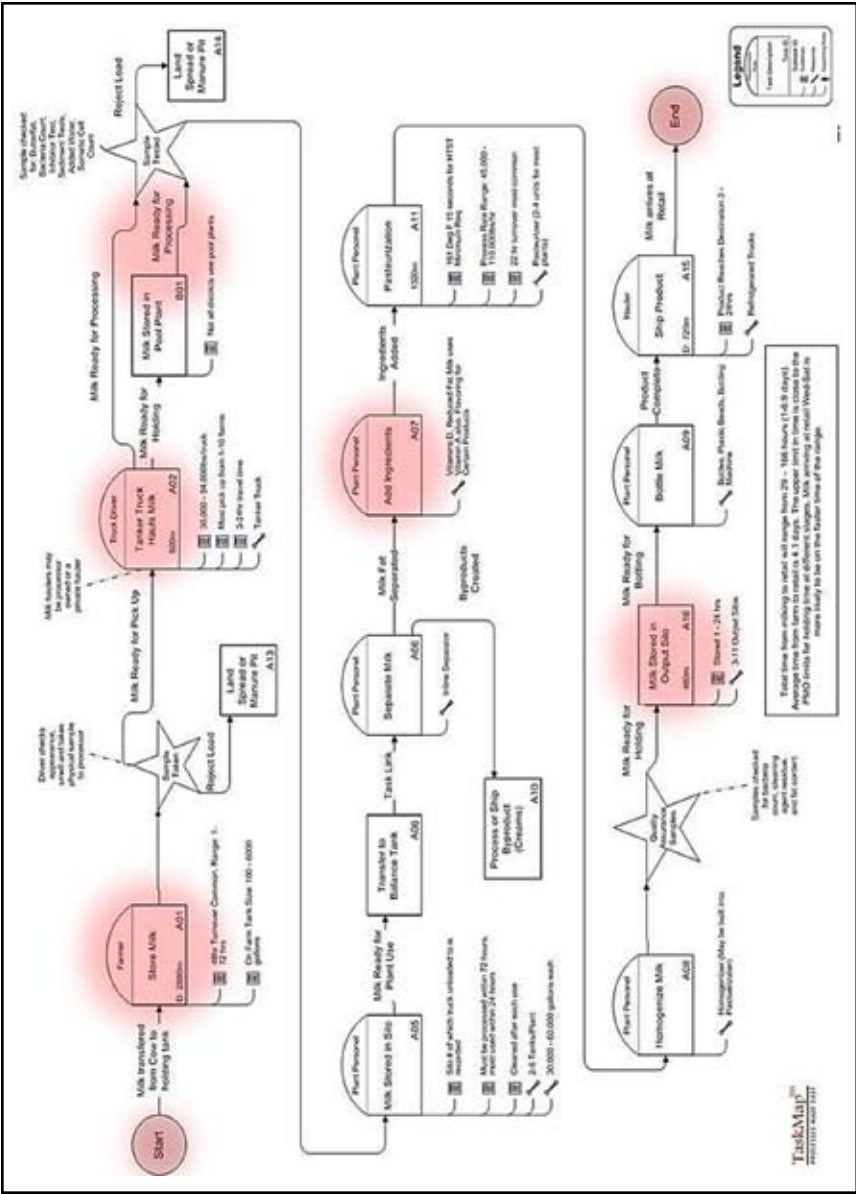


Figure 5. Minnesota fluid-milk flow diagram showing potential threat points—easy access at points of vulnerability presents possibilities of attack without detection and causing the most harm.

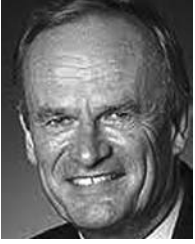
GENERAL INSIGHTS

The Department of Homeland Security has focused too broadly on too many risks, and I similarly fault our own center of excellence. We look at everything, whereas I think it would be wise to focus defenses on high-threat, -vulnerability and -consequence scenarios, radiological, nuclear and some chemical and biological. For other scenarios, it is useful to employ intelligence analysis and police work to intervene early or upstream rather than to defend. One of the undersecretaries of homeland security once said:

You are to find the bomber not the bomb.

With food, the objective should be to find risk-management options with large co-benefits that pay for themselves. For food defense, you might think in terms of strategies to prevent a terrorist tainting something that may be beneficial for other food-safety reasons. Equally, solutions that address regular safety issues by introducing new testing and inspection procedures may help prevent terrorism. Systems analysis and risk analysis have helped in the past, mostly to prevent the government from making stupid decisions, which is a worthy achievement. In one case, for example, we helped to avoid the implementation of laser-based counter-measures to be put on all commercial airplanes to prevent surface-to-air missile attacks, which would have cost \$30 billion dollars. We were partly responsible for that outcome.

The main challenge is how secure is secure enough? Clearly, we will never be completely safe from terrorism. Nor will we ever have a completely safe food supply. Because security measures increase dramatically when we get closer to zero risk, the cost goes up tremendously. Perhaps most importantly, increasing security creates other risks and inconveniences, and restricts civil liberties. We should always be aware of the need for a well balanced system, and avoid over-reacting in terms of security, thus compromising other values important to our society.



Detlof von Winterfeldt is the director of the International Institute for Applied Systems Analysis in Laxenburg, Austria. He is on leave from the University of Southern California (USC), where he is a professor of industrial and systems engineering and a professor of public policy and management.

Concurrently he is also visiting the London School of Economics and Political Science as a centennial professor in the Operational Research Group of the School of Management.

In 2003, Dr. Winterfeldt co-founded the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) at USC, the first university-based center of excellence funded by the US Department of Homeland Security; he served as CREATE's director until 2008.

For the past thirty years, he has been active in teaching, research, university administration, and consulting. He has taught courses in statistics, decision analysis, risk analysis, systems analysis, research design, and behavioral decision research. His research interests are in the foundation and practice of decision and risk analysis as applied to the areas of technology development, environmental risks, natural hazards and terrorism. He is the co-author of two books, two edited volumes, and (co)author of over a hundred journal articles and book chapters on these topics.